ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01
СОЗДАННОГО НА БАЗЕ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА
ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК, МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ, ПО ДИССЕРТАЦИИ
НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета 09.10.2018 г. № 1

О присуждении Браницкому Александру Александровичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 14 июня 2018 г., протокол № 1 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Браницкий Александр Александрович, 1990 года рождения, в 2012 г. с отличием окончил Санкт-Петербургский государственный университет по специальности «Математическое обеспечение и администрирование информационных систем» (диплом ОСА № 01802, рег. номер 0931030), в 2016 г. окончил очную аспирантуру в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук. Справка о сдаче кандидатских экзаменов № 13/203 выдана в 2016 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук (СПИИРАН). В настоящее время Браницкий Александр Александрович работает младшим научным сотрудником лаборатории проблем компьютерной безопасности в Федеральном государственном

бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН), Министерство науки и высшего образования.

Диссертация выполнена в лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН).

Научный руководитель – доктор технических наук, профессор КОТЕНКО Игорь Витальевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), главный научный сотрудник лаборатории проблем компьютерной безопасности.

Официальные оппоненты:

КОМАШИНСКИЙ Владимир Ильич, доктор технических наук, доцент, Институт проблем транспорта Российской академии наук им. Н.С. Соломенко, заместитель директора по научной работе;

ШЕРСТЮК Юрий Михайлович, доктор технических наук, доцент, АО «НИИ «Рубин», заместитель генерального конструктора

дали положительные отзывы на диссертацию.

Ведущая организация – Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»), г. Санкт-Петербург, в своем положительном отзыве, подписанном учёным секретарём ПАО «Интелтех», д.т.н., профессором Будко Павлом Александровичем, заместителем начальника отдела, к.т.н., доцентом Салюком Дмитрием Владиславовичем, начальником отдела, к.т.н. Бакаевым Михаилом Васильевичем и утвержденном первым заместителем генерального директора ПАО «Интелтех» по научной работе, к.т.н., доцентом Кулешовым Игорем Александровичем, указала, что диссертационная работа А.А. Браницкого представляет собой законченную научно-квалификационную работу, выполненную на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача, заключающаяся в разработке модельно-методического аппарата

для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта.

Соискателем разработана модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений, которая позволяет снизить количество конфликтных случаев классификации сетевых соединений за счет двухуровневой процедуры обучения иммунных детекторов; разработан алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений, который, в отличие от существующих, дополнен введением стратегий генетической оптимизации «мертвых» нейронов, что позволяет снизить время, затрачиваемое на настройку системы обнаружения атак; разработана методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений, позволяющая объединять такие разнородные средства обнаружения аномальных сетевых соединений, как сигнатурный анализ и методы вычислительного интеллекта; разработана архитектура и выполнена программная реализация распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа. Текст автореферата полностью соответствует содержанию диссертации. Диссертационное исследование «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» является научно-квалификационной работой и соответствует критериям, изложенным в п. 9 “Положения о присуждении ученых степеней”, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г., предъявляемым к кандидатским диссертациям, а его автор, Браницкий Александр Александрович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 21 опубликованную работу, в том числе по теме диссертации 21 работу, опубликованных в рецензируемых научных изданиях 9 работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ, – 6.

Основные научные результаты опубликованы в 21 научном труде общим объемом 11,0625 п.л., из которых 5 статей объемом 4,3125 п.л. выполнены в соавторстве, а 1 статья объемом 1,875 п.л. – лично. Наиболее значимые работы по теме диссертации:

1. Браницкий, А.А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А.А. Браницкий, И.В. Котенко // Информационно-управляющие системы. – 2015. – 4 (77). – С. 69–77. *Личный вклад соискателя – 90%.*
2. Браницкий, А.А. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений / А.А. Браницкий, И.В. Котенко // Проблемы информационной безопасности. Компьютерные системы. – 2015. – № 4. – С. 23–27. *Личный вклад соискателя – 90%.*
3. Браницкий, А.А. Анализ и классификация методов обнаружения сетевых атак / А.А. Браницкий, И.В. Котенко // Труды СПИИРАН. – 2016. – 2 (45). – С. 207–244. *Личный вклад соискателя – 90%.*
4. Браницкий, А.А. Иерархическая гибридизация бинарных классификаторов для выявления аномальных сетевых соединений / А.А. Браницкий // Труды СПИИРАН. – 2017. – 3 (52). – С. 204–233.
5. Браницкий, А.А. Открытые программные средства для обнаружения и предотвращения сетевых атак / А.А. Браницкий, И.В. Котенко // Защита Информации. Инсайд. – 2017. – 2 (74). – С. 40–47. *Личный вклад соискателя – 90%.*
6. Браницкий, А.А. Открытые программные средства для обнаружения и предотвращения сетевых атак (окончание) / А.А. Браницкий, И.В. Котенко // Защита Информации. Инсайд. – 2017. – 3 (75). – С. 58–66. *Личный вклад соискателя – 90%.*
7. Браницкий, А.А. Нейросетевой и иммуноклеточный подходы к распознаванию сетевых атак / А.А. Браницкий, А.В. Тимофеев // СПИСОК-2012. Материалы Всероссийской научной конференции по проблемам информатики. 25–27 апреля 2012 г. Санкт-Петербург. Т. 6. – Изд. "ВВМ", СПбГУ, 2012. – С. 335–340. *Личный вклад соискателя – 90%.*
8. Branitskiy, A. Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers / A. Branitskiy, I. Kotenko // In Proceedings of the 18th IEEE International Conference on Computational Science and Engineering (IEEE CSE2015). – IEEE. Oct. 2015. – Pp. 152–159. *Личный вклад соискателя – 80%.*
9. Branitskiy, A. Hybridization of computational intelligence methods for attack detection in computer networks / A. Branitskiy, I. Kotenko // Journal of Computational Science. – 2017. – Vol. 23. – Pp. 145–156. *Личный вклад соискателя – 80%.*

10. Branitskiy, A. Network Anomaly Detection Based on an Ensemble of Adaptive Binary Classifiers / A. Branitskiy, I. Kotenko // In Proceedings of International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. – Springer. 2017. – Pp. 143–157. *Личный вклад соискателя – 80%.*

Оригинальность содержания диссертации составляет не менее 95% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов, не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 7 отзывов, все отзывы положительны:

1) Общество с ограниченной ответственностью «Инновационный центр транспортных исследований». Отзыв составил доктор технических наук, старший научный сотрудник, И.О. генерального директора Чернов Владимир Юрьевич. Замечания: (1) На странице 12 говорится об извлечении 106 параметров, характеризующих сетевые соединения, однако не указана размерность сжатого вектора признаков, полученного в результате применения метода главных компонент. (2) Из текста автореферата непонятно, каким образом получен набор данных, содержащий три класса сетевых соединений (стр. 14), и что он из себя представляет.

2) Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Отзыв составил кандидат технических наук, доцент кафедры сетей связи и передачи данных СПБГУТ Пантюхин Олег Игоревич. Замечания: (1) Не обоснован выбор требований, предъявляемых к вычислительно интеллектуальным системам и в частности к разработанной системе обнаружения атак. (2) Не обоснован выбор ОС Linux в качестве платформы для проведения экспериментов.

3) Петербургский государственный университет путей сообщения императора Александра I. Отзыв составила кандидат технических наук, доцент Диасамидзе Светлана Владимировна. Замечания: (1) В автореферате недостаточно раскрыт вопрос целесообразности использования протокола RPC/SSL в качестве связующего звена между сенсорами и коллектором СОА. (2) На стр. 7 в начале последнего абзаца автор

указывает, что формулы (1) и (2) описывают разработанную модель искусственной иммунной системы, однако из них не видно тех особенностей, которые выделяют ее из существующих моделей. (3) Недостаточно освещены механизмы межъязыкового взаимодействия плагинов внутри интеллектуального ядра классификации объектов. (4) Недостаточно рассмотрены возможности внедрения вредоносного кода в ядро СОА за счет загрузки нелегитимных плагинов.

4) Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации». Отзыв составил доктор технических наук, профессор Иванов Александр Юрьевич. Замечания: (1) Из текста автореферата не вполне понятно, какие классы аномальных сетевых соединений рассматриваются в исследовании. (2) Недостаточно убедительно показано, за счет чего удалось добиться ускорения процесса обработки сетевых пакетов и снижения ресурсопотребления в разработанной системе обнаружения атак.

5) Военная академия связи имени Маршала Советского Союза С.М. Буденного. Отзыв составил кандидат технических наук, доцент Авраменко Владимир Семенович. Замечания: (1) В автореферате не описано функциональное предназначение каждого компонента разработанной СОА (рис. 3), в частности, опущено описание интерпретатора и менеджера классификаторов. (2) В автореферате не приведено обоснование выбора сети Кохонена для внутреннего представления иммунных детекторов. (3) Из автореферата не ясно, что автор использовал в качестве сетевых параметров в событийно-ориентированном анализаторе трафика.

6) «Концерн радиостроения «Вега» в г. Санкт-Петербурге. Отзыв составил доктор технических наук, профессор Оков Игорь Николаевич. Замечания: (1) Не определены характеристики аномальных сетевых соединений, что затрудняет оценку степени эффективности разработанного модельно-методического аппарата для их обнаружения. (2) Отсутствует сравнение разработанных предложений с моделями и алгоритмами, основанными на комбинированных подходах к обнаружению сетевых аномалий. (3) В автореферате цель исследования на страницах 4 и 7 сформулирована по-разному.

7) ОАО «Радиоавионика». Отзыв составил кандидат технических наук Попов Сергей Николаевич. Замечания: (1) В предлагаемой методике не учитывается наличие лица, принимающего решения в функциональном контуре принятия решений. (2) В автореферате отсутствуют функциональные представления критериев и показателей, предназначенных для оценки эффективности СОА. (3) В автореферате не соблюдены правила оформления алгоритмов, что делает их представление менее наглядным. (4) Не приведены репрезентативности статистик, на основе которых оценивались показатели эффективности, их доверительные интервалы и доверительные вероятности.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., доцент Комашинский В.И. является известным ученым и исследователем в области искусственных нейронных сетей, телекоммуникационных протоколов и технологий, систем передачи данных и информационной безопасности; д.т.н., доцент, Шерстюк Ю.М. является известным ученым и исследователем в области построения распределенных систем, телекоммуникационных сетей, разработки специального программного обеспечения и информационной безопасности; ведущая организация, Публичное акционерное общество «Информационные телекоммуникационные технологии», является известной в России организацией в области разработки автоматизированных систем связи, производства телекоммуникационного оборудования, а также создания систем защиты информации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны: оригинальные модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений, алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений, методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений, архитектура и программная реализация распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа.

предложены:

модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений, в которой, в отличие от существующих, реализованы двухуровневый алгоритм обучения иммунных детекторов и автоматическое вычисление порога их активации, что позволяет повысить уровень корректности классификации аномальных сетевых соединений и снизить уровень ложных срабатываний.

алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений, который отличается введением нескольких стратегий генетической оптимизации весовых коэффициентов нейронов, что позволяет снизить время настройки детекторов системы обнаружения атак;

методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений, которая, в отличие от существующих, обеспечивает «ленивое» подключение бинарных классификаторов и позволяет выполнять многоуровневый анализ векторов признаков сетевых соединений при помощи сигнатурного анализа и методов вычислительного интеллекта с распределением задач между сенсорами и коллектором;

архитектура распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа, в которой, в отличие от существующих, реализована оригинальная методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений, а также добавлена поддержка «горячей» вставки нового исполняемого кода, содержащего функционирование и структуру классификатора.

доказана перспективность использования разработанной методики для построения распределенных гибридных систем обнаружения атак;

введены:

- схема классификации методов обнаружения атак в компьютерных сетях;
- требования, предъявляемые к функционированию вычислительно интеллектуальных сетевых систем обнаружения атак;

- рекомендации по применению разработанного модельно-методического аппарата для построения систем обнаружения атак

Теоретическая значимость исследования обоснована тем, что:

доказаны теоретические утверждения о применимости разработанных модели, алгоритма и методики к процессу обнаружения аномальных сетевых соединений, которые позволяют повысить эффективность функционирования системы обнаружения атак;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы аппарат и методы теории вероятностей, теории множеств, теории вычислительного интеллекта, теории формальных языков, теории защиты информации;

изложены методологические и методические основы использования задачи обучения и применения коллектива разнородных адаптивных классификаторов для построения алгоритмов и систем обнаружения атак;

раскрыты

место и роль методов вычислительного интеллекта в областях искусственного интеллекта и обнаружения аномальных сетевых соединений;

основные вопросы, связанные с ограничениями и применимостью сигнатурных и эвристических механизмов обнаружения атак в компьютерных сетях;

возможность применения комбинированного подхода, сочетающего разнородные адаптивные классификаторы вычислительного интеллекта и сигнатурный анализ, к обнаружению аномальных сетевых соединений;

изучены существующие методы обнаружения сетевых атак, алгоритмов обучения адаптивных классификаторов и методов построения коллектива классификаторов, при этом особое внимание уделено рассмотрению вопросов применимости бинарных классификаторов к решению задачи обнаружения аномальных сетевых соединений;

проведена модернизация схемы классификации существующих методов обнаружения сетевых атак, включая методов обнаружения аномалий и методов обнаружения злоупотреблений.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

• модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений;

• алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;

• методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;

• архитектура и программная реализация распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа;

внедрены в учебный процесс в технологическом институте Блекинге (Карлскруна, Швеция) при подготовке курса “Современная сетевая и облачная безопасность” для обучения магистров в университетах-партнерах:

• методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;

• архитектура и программная реализация распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа;

используются кафедрой Защищенных систем связи СПбГУТ в учебном процессе на старших курсах обучения студентов по направлению подготовки бакалавров 10.03.01 “Информационная безопасность” по дисциплинам “Программно-аппаратные средства обеспечения информационной безопасности” и “Основы информационной безопасности” при чтении курсов лекций, проведении практических и лабораторных работ:

• модель искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений;

• алгоритм генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;

используются на кафедре проектирования и безопасности компьютерных систем ИТМО в учебном процессе при подготовке магистров по направлению 10.04.01 “Информационная безопасность” по дисциплинам “Методология информационной безопасности” и “Основы форензики” при чтении курсов лекций, проведении практических и лабораторных работ.

определены возможности и перспективы практического применения полученных результатов диссертационного исследования при построении распределенных систем обнаружения атак;

создана система обнаружения атак, характеризующаяся двухуровневым механизмом анализа сетевой активности за счет наличия сенсоров, выполняющих первичную обработку низкоуровневых данных (пакетов), и коллектора, предназначенного для обработки агрегированных сетевых потоков;

представлены направления для дальнейших научных исследований, в основе которых может быть использован разработанный модельно-методический аппарат.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ

достоверность полученных результатов подтверждена проведением тщательного анализа работ по выбранной теме исследования, корректным применением научно-методического аппарата, апробацией основных результатов диссертации в виде печатных трудов и докладов на международных и российских конференциях, наличием актов о внедрении результатов диссертационной работы;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования и согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области обнаружения аномальных сетевых соединений и построения сетевых систем обнаружения атак;

использованы полученные экспериментальные характеристики разработанной системы обнаружения атак для сравнения с данными, приведенными в современной научной и технической литературе по обнаружению сетевых атак;

установлено качественное и количественное соответствие результатов решения задачи разработки модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта. При этом подтверждено преимущество разработанного подхода перед результатами, полученными другими авторами, путем проведения множества разнообразных экспериментов.

использованы современные методы сбора, обработки исходной информации и формирования обучающих выборок, алгоритмы обучения классификаторов и построения коллектива классификаторов с приложением к обнаружению аномальных сетевых соединений.

Личный вклад соискателя состоит в:

- анализе современного состояния исследований в области обнаружения сетевых атак и аномальных сетевых соединений;
- классификации методов обнаружения сетевых атак;
- постановке задачи разработки модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта;
- разработке программных инструментов для тестирования сетевых систем обнаружения атак и оценке их возможностей;
- разработке модели искусственной иммунной системы на базе эволюционного подхода для классификации сетевых соединений;
- разработке алгоритма генетико-конкурентного обучения сети Кохонена для обнаружения аномальных сетевых соединений;
- разработке методики иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений;
- разработке архитектуры и программной реализации распределенной системы обнаружения атак, построенной на основе гибридизации методов вычислительного интеллекта и сигнатурного анализа;
- разработке программного стенда для генерации сетевых атак и экспериментальной оценке разработанной системы обнаружения атак;

- подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Браницкий А.А. в своей диссертационной работе решил научную задачу разработки модельно-методического аппарата для обнаружения аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта, имеющую важное социально-экономическое и хозяйственное значение.

На заседании 09.10.2018 г. диссертационный совет принял решение присудить Браницкому А.А. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 21 человека, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 21, против нет, недействительных бюллетеней нет.

Председатель
доктор технич
член-корресп Юсупов Рафаэль Мидхатович

Ученый секр
кандидат тех Зайцева Александра Алексеевна
09.10.2018 г.